What is claimed is:

1. A method for maintaining computer security, comprising:

providing a database of known good software;

opening a file;

identifying the file being opened;

determining whether an entry exists in the database of known good software for the identified file; and

performing at least one of allowing and preventing the opening of the file from continuing based on the result of the determination.

2. The method of claim 1, wherein the file comprises an executable file.

3. The method of claim 2, wherein the executable file comprises an application.

4. The method of claim 1, wherein identifying the file being opened comprises determining a unique value of the file, the unique value being a hash value generated according to a hashing algorithm and comparing the unique value to entries in the database of known good software.

5. The method of claim 4, wherein the performing at least one of allowing and preventing the opening of the file from continuing comprises allowing the file to continue to be opened if it is determined that the determined unique value corresponds to an entry in the

database of known good software.

6. The method of claim 1, further comprising providing a database of unfamiliar software and determining whether an entry exists in the database of unfamiliar software for the identified file.

7. The method of claim 6, further comprising providing date stamp information for each entry in the database for unfamiliar processes indicating a date on which the entry was first made.

8. The method of claim 6, further comprising providing a value for each entry in the database for unfamiliar software indicating a number of times a file corresponding to the entry was opened.

9. The method of claim 8, wherein the value comprises the number of times an executable in a file has been executed.

10. The method of claim 7, further comprising determining an amount of time an entry has been in the database for unfamiliar processes by comparing the date stamp information with a current date.

11. The method of claim 10, further comprising moving an entry from the database for unfamiliar software to the database for known good software if it is determined that the

entry has been in the database for unfamiliar software for a sufficient period of time.

12. The method of claim 6, further comprising adding an entry to the database of unfamiliar software if an entry for the file being opened is not found in at least one of the database for known good software and the database for unfamiliar software.

13. The method of claim 6, further comprising placing at least one operating system call hook if it is determined that an entry exists in the database for unfamiliar software.

14. The method of claim 13, wherein the operating system call hook notifies a Trojan notification service that a file corresponds to an entry in the database for unfamiliar software.

15. The method of claim 14, wherein the Trojan notification service prompts a user for input regarding whether the operating system call should be passed along..

16. The method of claim 15, wherein opening of the file is allowed to proceed if the operating system call is passed along.

17. A system for maintaining computer security, comprising:

a database of known good software;

a system for opening a file;

a system for identifying the file being opened;

a system for determining whether an entry exists in the database of known good

software for the identified file; and

a system for performing at least one of allowing and preventing the opening of the file from continuing based on the result of the determination.

18. The system of claim 17, wherein the file comprises an executable file.

19. The system of claim 18, wherein the executable file comprises an application.

20. The system of claim 17, wherein the system for identifying the file being opened comprises a system for determining a unique value of the file, the unique value being a hash value generated according to a hashing algorithm and a system for comparing the unique value to entries in the database of known good software.

21. The system of claim 20, wherein the system for performing at least one of allowing and preventing the opening of the file from continuing comprises a system for allowing the file to continue to be opened if it is determined that the determined unique value corresponds to an entry in the database of known good software.

22. The system of claim 17, further comprising a database of unfamiliar software; and

a system for determining whether an entry exists in the database of unfamiliar software for the identified file.

23. The system of claim 22, further comprising a system for providing date stamp information for each entry in the database for unfamiliar processes indicating a date on which the entry was first made.

24. The system of claim 22, further comprising a system for providing a value for each entry in the database for unfamiliar software indicating a number of times a file corresponding to the entry was opened.

25. The system of claim 24, wherein the value comprises the number of times an executable in a file has been executed.

26. The system of claim 23, further comprising a system for determining an amount of time an entry has been in the database for unfamiliar processes by comparing the date stamp information with a current date.

27. The system of claim 26, further comprising a system for moving an entry from the database for unfamiliar software to the database for known good software if it is determined that the entry has been in the database for unfamiliar software for a sufficient period of time.

28. The system of claim 22, further comprising a system for adding an entry to the database of unfamiliar software if an entry for the file being opened is not found in at least one of the database for known good software and the database for unfamiliar software.

29. The system of claim 22, further comprising a system for placing at least one operating system call hook if it is determined that an entry exists in the database for unfamiliar software.

30. The system of claim 29, wherein the operating system call hook notifies a Trojan notification service that a file corresponds to an entry in the database for unfamiliar software.

31. The system of claim 30, wherein the Trojan notification service prompts a user for input regarding whether the operating system call should be passed along..

32. The system of claim 31, wherein opening of the file is allowed to proceed if the operating system call is passed along.

33. A computer recording medium including computer executable code for maintaining computer security, comprising:

code for providing a database of known good software;

code for opening a file;

code for identifying the file being opened;

code for determining whether an entry exists in the database of known good software for the identified file; and

code for performing at least one of allowing and preventing the opening of the file from continuing based on the result of the determination.

34. The computer recording medium of claim 33, wherein the file comprises an executable file.

35. The computer recording medium of claim 34, wherein the executable file comprises an application.

36. The computer recording medium of claim 33, wherein the code for identifying the file being opened comprises code for determining a unique value of the file, the unique value being a hash value generated according to a hashing algorithm and code for comparing the unique value to entries in the database of known good software.

37. The computer recording medium of claim 36, wherein the code for performing at least one of allowing and preventing the opening of the file from continuing comprises code for allowing the file to continue to be opened if it is determined that the determined unique value corresponds to an entry in the database of known good software.

38. The computer recording medium of claim 33, further comprising code for providing a database of unfamiliar software and code for determining whether an entry exists in the database of unfamiliar software for the identified file.

39. The computer recording medium of claim 38, further comprising code for providing date stamp information for each entry in the database for unfamiliar processes

indicating a date on which the entry was first made.

40. The computer recording medium of claim 38, further comprising code for providing a value for each entry in the database for unfamiliar software indicating a number of times a file corresponding to the entry was opened.

41. The computer recording medium of claim 40, wherein the value comprises the number of times an executable in a file has been executed.

42. The computer recording medium of claim 39, further comprising code for determining an amount of time an entry has been in the database for unfamiliar processes by comparing the date stamp information with a current date.

43. The computer recording medium of claim 42, further comprising code for moving an entry from the database for unfamiliar software to the database for known good software if it is determined that the entry has been in the database for unfamiliar software for a sufficient period of time.

44. The computer recording medium of claim 38, further comprising code for adding an entry to the database of unfamiliar software if an entry for the file being opened is not found in at least one of the database for known good software and the database for unfamiliar software.

45. The computer recording medium of claim 38, further comprising code for placing at least one operating system call hook if it is determined that an entry exists in the database for unfamiliar software.

46. The computer recording medium of claim 45, wherein the operating system call hook notifies a Trojan notification service that a file corresponds to an entry in the database for unfamiliar software.

47. The computer recording medium of claim 46, wherein the Trojan notification service prompts a user for input regarding whether the operating system call should be passed along..

48. The computer recording medium of claim 47, wherein opening of the file is allowed to proceed if the operating system call is passed along.